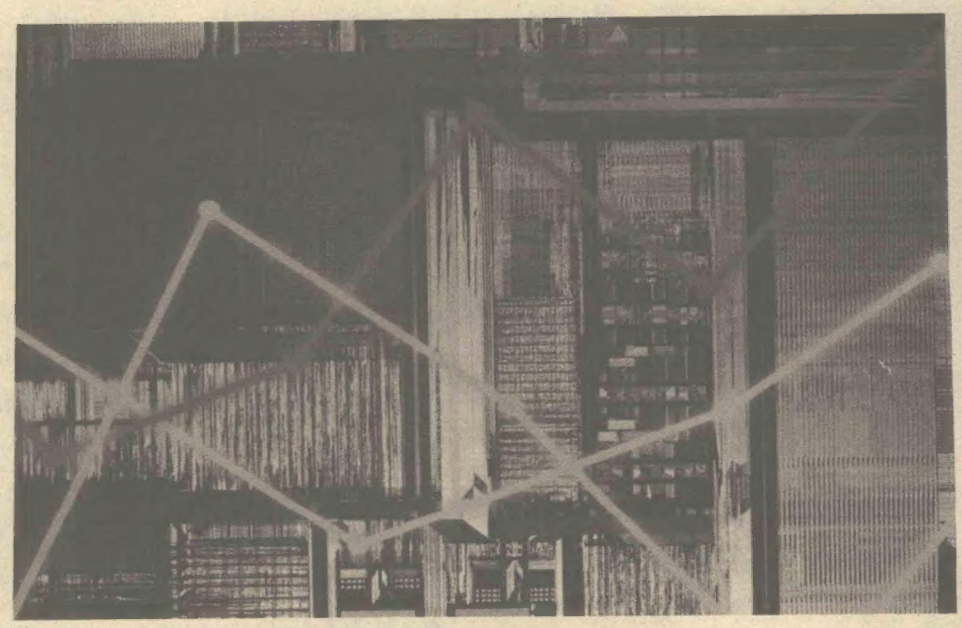
มุมนักเล่น

NETWORKING

เขมะทัต วิภาตะวนิช

สื่อสารข้อมูลโดยใช้ชุดโปรโตคอล TCP/IP ตอนที่ 1

เปิดคอลัมน์ใหม่ กล่าวถึงระบบสื่อสารข้อมูล โดยใช้โปรโตคอล TCP/IP เป็นตัวจักรสำคัญในการรับส่งหรือโอนถ่ายข้อมูล



สวัสดีครับท่านผู้นิยมการอ่านทุกท่าน คอลัมน์ที่ท่านกำลังอ่านอยู่นี้คือคอลัมน์เน็ตเวอร์กกิง ซึ่งเป็นคอลัมน์เปิดใหม่ มีวัตถุประสงค์ให้ผู้อ่านมีความรู้ความเข้าใจระบบเครือข่ายที่ใช้งานอยู่ในปัจจุบันและที่กำลังจะเกิดขึ้นในอนาคต ทำให้สามารถออกแบบระบบเครือข่ายโดยใช้วิจารณญาณของตนเองได้ สามารถแยกแยะข้อดีข้อเสียของอุปกรณ์ที่จะนำมาใช้กับระบบเครือข่ายได้ และสามารถแก้ไขปัญหาที่เกิดขึ้นในระบบเครือข่ายได้ ทางด้านเนื้อหานั้นก็จะประกอบด้วยภาคทฤษฎีและภาคปฏิบัติเพื่อให้ผู้อ่านสามารถนำทฤษฎีไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ รายละเอียดของเนื้อหาจะมีตั้งแต่สื่อนำสัญญาณไปจนถึงโปรแกรมประยุกต์ ประเภทของอุปกรณ์เฉพาะทางที่ถูกนำมาใช้ในระบบเครือข่าย เช่น บริดจ์ (bridge) อุปกรณ์หาเส้นทาง (router) ชุดของโปรโตคอลมาตรฐานต่าง ๆ ที่สำคัญ และอื่น ๆ อีกมากมาย

สำหรับประเทศไทยในขณะนี้ไม่ว่าจะเป็นภาครัฐบาล ภาคเอกชน หรือแม้กระทั่งบุคคลธรรมดาก็มีการตื่นตัวอย่างมากทางด้านเน็ตเวอร์ก ตัวอย่างหนึ่งที่ประจักษ์ชัดและเป็นที่ยอมรับกันโดยทั่ว

ไปคือ การเชื่อมต่อเครือข่ายสื่อสารข้อมูลในประเทศไทยเข้ากับเครือข่ายอินเตอร์-เน็ต หรือที่เรียกกันอย่างสุดหรูว่าเครือข่ายโลกาภิวัตน์ ซึ่งเป็นขุมทรัพย์และแหล่งแลกเปลี่ยนข้อมูลอันประเมินค่ามิได้

การเปิดตัวของคอลัมน์นี้เป็นการเบิกโรงด้วยการกล่าวถึงเบื้องหลังความสำเร็จของเครือข่ายอินเตอร์เน็ต โดยบทความนี้มีความยาวสองตอน เน้นเนื้อหาหลักทางด้านชุดโปรโตคอล TCPIP อย่างคร่าว ๆ สำหรับรายละเอียดในส่วนต่าง ๆ ของชุดโปรโตคอลนี้ผู้เขียนจะค่อย ๆ ลำดับมาเล่าสู่กันฟัง อย่างไรก็ตาม สิ่งที่พวกเราต้องการอย่างมากก็คือความคิดเห็นของท่านผู้อ่านที่มีต่อคอลัมน์นี้ ไม่ว่าจะเป็นแง่บวกหรือลบก็ช่วยกันเขียนเข้ามามาก ๆ นะครับ เพราะพวกเรามีคติว่าการแสดงความคิดเห็นของพวกท่านก็คือการปรับปรุงคุณภาพของชิ้นงาน

ท่านผู้อ่านที่คุ้นเคยกับเครือข่ายอินเตอร์เน็ต (Internet) ก็คงจะคุ้นเคยกับชุดโปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) เช่นกัน เพราะเครือข่ายอินเตอร์เน็ตซึ่งอุดมไปด้วยทรัพยากรอันมหาศาลและเอื้ออำนวยประโยชน์ต่อผู้ใช้นานัปการต้องอาศัยชุดโปรโตคอล TCP/IP ในการส่งผ่านข้อมูลทั้งสิ้น (อนึ่ง การเรียกชุดโปรโตคอล TCP/IP เพียงอย่างเดียวย่อมไม่ถูกต้องนัก ที่ถูกต้องทั้งหมดควรจะเรียกว่า ชุดโปรโต-คอล TCP & UDP/IP แต่เนื่องจากว่าโปรโตคอล TCP มีความสามารถให้บริการสูงกว่า UDP (User Datagram Protocol) ประกอบกับโดยทั่วไปเรียกเฉพาะ TCP/IP ดังนั้นผู้เขียนจึงขออนุญาตยึดถือขนบธรรมเนียมประเพณีแบบเดิมคือเรียกเฉพาะ TCP/IP แต่รวมความหมายไปถึง UDP/IP ด้วย)

ประวัติความเป็นมาของชุดโปร-

โตคอล TCP/IP สืบเนื่องมาจากแนวความคิดของกระทรวงกลาโหมของประเทศสหรัฐอเมริกาที่ต้องการเชื่อมต่อเครื่องคอมพิวเตอร์ที่มีอยู่มากมายหลายยี่ห้อเข้าด้วยกันเป็นระบบเครือข่ายเดียว โดยมอบหมายให้ DARPA (Defense Advanced Research Project Agency, ซึ่งแต่เดิมเรียกว่า ARPA) เป็นผู้รับผิดชอบ ในช่วงฤดูใบไม้ร่วงปี ค.ศ. 1969 นับเป็นจุดเริ่มต้นของชุดโปรโตคอล TCP/IP เพราะมีการแสดงให้เห็นถึงการเชื่อมต่อเครื่องคอมพิวเตอร์จาก 4 แห่งเข้าหากัน ซึ่งประกอบไปด้วย U. of California at Los Angeles (UCLA), Stanford Research Institute (SRI), U. of California at Santa Barbara (UCSB) และ U. of Utah โดยเรียกเครือข่ายนี้ว่า ARPANET และมีบริษัท Bolt Beranek and Newman (BBN) เป็นผู้ดูแลการเชื่อมโยงเข้าหากัน รูปแบบการสื่อสารข้อมูลใช้เทคนิคของการสวิตช์กลุ่มข้อมูล (packet switching) คือการส่งข้อมูลจากเครื่องคอมพิวเตอร์ต้นทางผ่านโหนดข้างเคียงไปจนถึงปลายทาง

ในปี ค.ศ. 1972 เป็นการสาธิตความสามารถของระบบเครือข่ายเป็นครั้งแรก โดยมีเครื่องคอมพิวเตอร์จำนวน 50 เครื่องต่อเข้ากับระบบที่มีอุปกรณ์สวิตช์กลุ่มข้อมูลทำหน้าที่ส่งผ่านข้อมูลระหว่างเครื่องคอมพิวเตอร์ (อุปกรณ์สวิตช์กลุ่มข้อมูลนี้ ARPANET เรียกว่า Interface Message Processor (IMP) ในช่วงต้นทศวรรษที่ 80 ชุดโปรโตคอล TCP/IP ได้ถูกรวมเข้าเป็นความสามารถหนึ่งของระบบดำเนินการยูนิกซ์ภายใต้ชื่อ UNIX BSD 4.2 เพื่อความปลอดภัยของข้อมูลทางทหาร DARPA จึงได้ทำการแบ่งเครือ-ข่าย ARPANET ออกเป็น 2 เครือข่ายคือ เครือข่ายทางด้านพลเรือนและงานวิจัย ซึ่งยังคงใช้ชื่อ ARPANET ตามเดิม และเครือข่ายทางทหารใช้ชื่อว่า MILNET นับตั้งแต่นั้นมาจนถึงปัจจุบันระบบสื่อสารข้อมูลโดยใช้ชุดโปรโตคอล TCP/IP ก็เป็นที่ยอมรับแก่คนทั่วไป จนกลายเป็นมาตร-ฐานแบบที่เรียกว่า "de facto"

สำหรับบทความนี้เป็นการกล่าวถึงระบบสื่อสารข้อมูลคอมพิวเตอร์โดยใช้ชุดโปรโตคอล TCP/IP เป็นตัวจักรสำคัญในการรับส่งหรือถ่ายโอนข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่อาจจะอยู่ในระบบเครือข่ายเดียวกันหรือต่างกันก็ได้ ซึ่งหมายความว่าชุดโปรโตคอล TCP/IP นี้สามารถสนับสนุนได้ทั้งระบบเครือข่ายเฉพาะบริเวณ (Local Area Network (LAN) และเครือข่ายบริเวณกว้าง (Wide Area Network (WAN) ประเด็นสำคัญในการออกแบบระบบสื่อสารข้อมูลเพื่อทำให้ระบบไร้ซึ่ง "ตะเข็บหรือรอยต่อ" ต้องอาศัยความเข้าใจความสัมพันธ์ของโปร-โตคอลอย่างลึกซึ้ง ซึ่งจะเป็นเหตุนำไปสู่การเลือกใช้หรือสนับสนุนโปรแกรมประ-ยุกต์ของผู้ใช้งาน การเลือกใช้อุปกรณ์ในระบบเครือข่าย เช่น อุปกรณ์หาเส้นทาง (router) หรืออุปกรณ์บริดจ์ เป็นต้น การกำหนดหมายเลขของเครื่องคอมพิวเตอร์

(host)ภายในระบบ การเลือกใช้พอร์ตในการเชื่อมต่อให้เหมาะสม เช่น WAN หรือ LAN เป็นต้น ตลอดจนการใช้สื่อนำสัญญาณซึ่งจะเป็นผลทำให้ระบบทั้งหมดพร้อมที่จะรองรับต่อการขยายตัวและเทคโนโลยีใหม่ในอนาคต

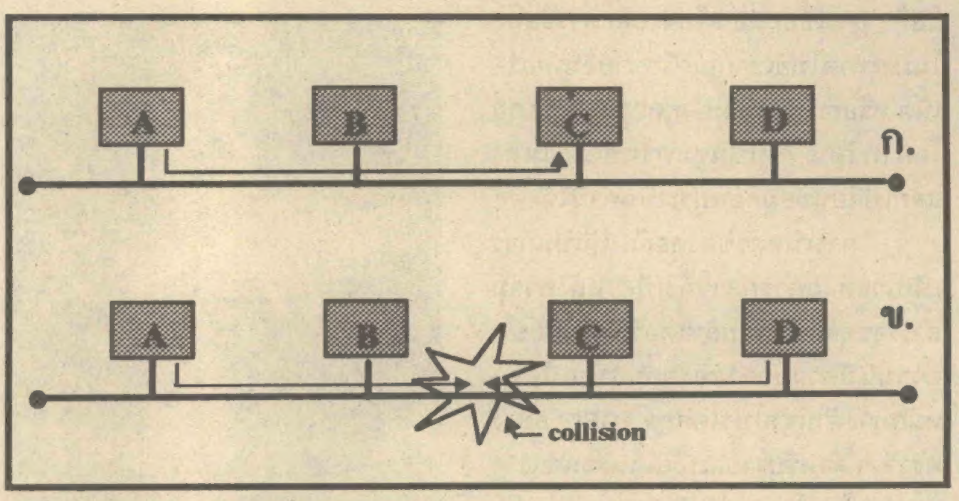
ในที่นี้จะไม่ขอกล่าวถึงรูปแบบมาตรฐานของ ISO (International Organization for Standardization) เพราะผู้เขียนเคยกล่าวไว้แล้วในวารสารไมโครฯ ฉบับที่ 81 ในบทความเรื่อง "มารู้จักมาตรฐานระบบเครือข่ายคอมพิวเตอร์"

อย่างไรก็ตาม การที่จะเข้าใจความสามารถของชุดโปรโตคอล TCP/IP ซึ่งเป็นโปรโตคอลในชั้นที่ 4 และ 3 ตามลำดับได้อย่างถ่องแท้นั้นจำเป็นที่จะต้องกล่าวถึงโปรโตคอลในชั้นที่ 2 เสียก่อน เพราะเป็นส่วนที่อยู่ติดกัน และในที่นี้จะขอยกกรณีระบบแลนที่ใช้โปรโตคอลชั้นที่ 2 เป็นอีเธอร์เนต (ethernet) และ โทเก้นริง (token ring) มาอธิบายเพื่อให้เข้าใจถึงความแตกต่างของระบบแลนทั้งสองประเภท หลังจากนั้นก็จะอธิบายว่าทำไมในระบบแลนที่แตกต่างกันจึงสามารถเชื่อมโยงงานประยุกต์เข้าหากันได้โดยใช้ชุดโปรโตคอล TCP/IP

ประเภทของเครือข่าย

ระบบเครือข่ายสื่อสารข้อมูลแบ่งได้เป็น 2 ประเภทใหญ่ ๆ คือ เครือข่ายเฉพาะบริเวณ และเครือข่ายบริเวณกว้าง

เครือข่ายประเภทแรกมุ่งประเด็นการให้บริการที่อัตราเร็วในการส่งผ่านข้อมูลสูงมากคือตั้งแต่ 4 เมกะบิตต่อวินาทีขึ้นไป มีรัศมีทำการอยู่ในช่วงประมาณ 2-10 กิโลเมตร และผู้ที่ลงทุนก็คือเจ้าของระบบนั่นเอง ไม่ว่าจะเป็นรัฐหรือเอกชนก็ตาม



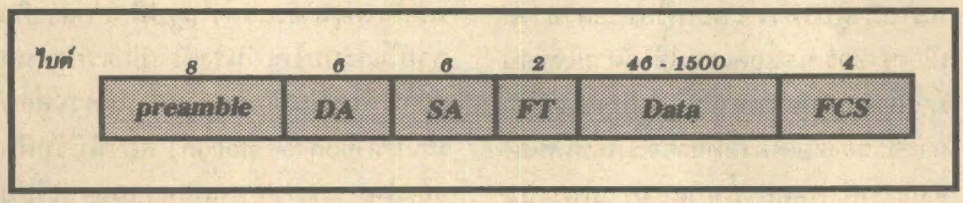
รูปที่ 1 ก. การส่งผ่านข้อมูลที่ไม่เกิดการชนกัน
ข. การส่งผ่านข้อมูลที่เกิดการชนกัน

เครือข่ายประเภทที่สองมุ่งประเด็นการให้บริการระยะไกล เช่น ภายในตัวจังหวัดหรือระหว่างประเทศ เป็นต้น โดยมีรัศมีทำการอยู่ประมาณ 8 กิโลเมตรขึ้นไป แต่ในแง่อัตราเร็วของข้อมูลไม่สูงมากนักคืออยู่ในช่วงประมาณ 1.2 - 2048 กิโลบิตต่อวินาที โดยมีหน่วยงานของรัฐหรือเอกชนที่ได้รับสัมปทานเป็นผู้ดูแลหรือเป็นเจ้าของระบบ

อนึ่ง ความหมายของเครือข่ายทั้งสองประเภทที่กล่าวถึงข้างต้นเป็นเพียงการกำหนดอย่างคร่าว ๆ ซึ่งในทางปฏิบัติอาจเบี่ยงเบนได้บางประการ

อีเธอร์เนตแลน

ระบบแลนในปัจจุบันมีส่วนหนึ่งที่เหมือนกันคือ การใช้แบนวิดธ์ (bandwidth) และสื่อนำสัญญาณ (media) ร่วมกัน แลนในแต่ละประเภทหรือแต่ละมาตรฐานจะมีความแตกต่างหลักคือ รูปแบบของโปรโตคอลที่ใช้ในการสื่อสารข้อมูล และวิธีการในการเข้าใช้ช่องสัญญาณในการส่งผ่านข้อมูล สำหรับอีเธอร์เนตอาศัยวิธีการที่เรียกว่า "CSMA/CD (Carrier Sense Multiple Access with Collision Detection)" ดังแสดงในรูปที่ 1 กล่าวคือ ก่อนที่สถานีใดจะส่งข้อมูล ต้องทำการฟังหรือตรวจสอบสื่อนำสัญญาณเสียก่อนว่ามีสถานีอื่นใช้อยู่หรือไม่ ถ้ามีก็จะคอยไปจนกว่าสื่อนำสัญญาณจะว่างลงแล้วจึงส่งข้อมูลออกไป แต่ถ้าในตอนแรกพบว่าว่างก็สามารถส่งข้อมูลได้ทันที ขณะที่สถานีหนึ่ง ๆ ทำการส่งข้อมูลอยู่ก็จะทำการตรวจสอบสื่อนำสัญญาณไปพร้อม ๆ กัน เพื่อดูว่าระดับแรงดันของสัญญาณผิดแผกแตกต่างไปจากระบบปกติหรือไม่ ถ้าไม่ผิดปกติตลอดช่วงของการส่งข้อมูล สถานีที่ส่งข้อมูลก็สรุปว่าข้อมูลได้ไปถึงปลายทางเรียบร้อยแล้ว พร้อมกับออกจากการเข้าครอบครองสื่อนำสัญญาณ แต่ถ้าไม่เป็นระดับปกติ แสดงว่าเกิดการชนกันของข้อมูล ดังนั้นทุก ๆ สถานีที่กำลังส่งข้อมูลอยู่ในขณะนั้นต้องหยุดการส่งข้อมูลและออกจากการเข้าครอบครองสื่อนำสัญญาณโดยทันที และพร้อมกันนั้นก็สุ่มหาเวลาตามขั้นตอนวิธีของ "binary back off" เพื่อใช้ในการกำหนดการเข้าใช้ช่องสัญญาณในเวลาต่อไป



รูปที่ 2 เขตต่าง ๆ ภายในอีเธอร์เนตเฟรม

อนึ่ง ในเวลาหนึ่ง ๆ จะมีเพียงสถานีเดียวเท่านั้นที่สามารถใช้ช่องสัญญาณในระบบอีเธอร์เนตแลน สำหรับรูปแบบเฟรมของอีเธอร์เนตแสดงในรูปที่ 2 ประกอบด้วย 6 เขตคือ

เขตแนะนำตัว (preamble) มีรหัสคงที่ $(AA)_H$ ขนาด 7 ไบต์เพื่อใช้ในการเข้าจังหวะระหว่างสถานีส่งและสถานีรับข้อมูล แต่สำหรับไบต์สุดท้ายมีรหัสคือ $(AB)_H$ ใช้ในการบอกถึงจุดเริ่มต้นของเขต DA

เขตแอดเดรสปลายทาง (destination address) มีขนาด 6 ไบต์ ใช้บอกถึงแอดเดรสของสถานีปลายทางที่ต้องการส่งข้อมูลไปให้ แต่ถ้าต้องการให้ข้อมูลไปถึงทุก ๆ สถานีโดยใช้เฟรมเดียวจะใช้แอดเดรสพิเศษที่เรียกว่า แอดเดรสกระจายข่าว (broadcast address) มีรหัสคงที่คือ $(FH)_H$ ทุกไบต์ แอดเดรสประเภทนี้มีข้อดีคือ สมมติว่าในระบบมี 1 สถานีที่ต้องการส่งข้อมูลไปยัง 9 สถานีที่เหลืออยู่ในระบบ แทนที่จะต้องส่งถึง 9 เฟรมกลับใช้เพียงแค่ 1 เฟรมเท่านั้นทั้ง 9 สถานีก็รับข้อมูลได้เหมือนกัน ซึ่งเป็นการประหยัดช่วงเวลาในการส่งผ่านข้อมูล ทำให้เวลาที่เหลือนำไปใช้ในการส่งผ่านข้อมูลอื่น ๆ ได้

เขตแอดเดรสต้นทาง (source address) มีขนาด 6 ไบต์ ใช้บอกถึงสถานีต้นทางที่เป็นเจ้าของอีเธอร์เนตเฟรม แอดเดรสนี้มีประโยชน์ต่ออุปกรณ์บริดจ์เป็นอย่างมาก

เขตประเภทของเฟรม (frame type) มีขนาด 2 ไบต์ ใช้บอกถึงชนิดของโปรโตคอลที่ถูกบรรจุอยู่ในเขตข้อมูล เช่น ถ้าเป็นโปรโตคอล IPX (Internetwork Packet Exchange) เขต FT จะมีค่า $(8137,8138)_H$ แต่ถ้าเป็นโปรโตคอล IP จะมีค่า $(0800)_H$ เป็นต้น

เขตข้อมูล เป็นส่วนที่ใช้ในการบรรจุข้อมูลหรือโปรโตคอลที่อยู่ในชั้นที่ 2 หรือสูงกว่า มีความยาวอยู่ในช่วง 46-1500 ไบต์

เขตตรวจสอบความผิดพลาดของข้อมูล (frame check sequence) มีขนาด 4 ไบต์ ใช้หลักการของ CRC (cyclic redundancy code) ในการตรวจสอบหาความผิดพลาดของข้อมูล เพื่อที่ว่าปลายทางจะได้ไม่นำข้อมูลที่ผิดพลาดไปประมวลผล เมื่อปลายทางตรวจพบความผิดพลาดก็จะแจ้งไปยังสถานีต้นทางให้ส่งข้อมูลชุดเดิมกลับมาใหม่อีกครั้งหนึ่ง วิธีการในการตรวจสอบเช่นเดียวกับที่ใช้ในโปรโตคอล HDLC (High-level Data Link Control) แต่ใช้ลำดับของสมการในการตรวจสอบต่างกัน ซึ่งในที่นี้ใช้สมการ

$$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X1$$

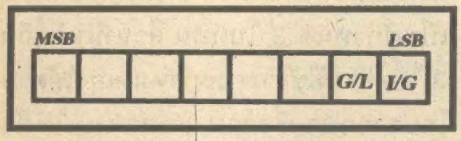
อนึ่ง แอดเดรสที่ถูกบรรจุอยู่ในโปรโตคอลอีเธอร์เนตถูกกำหนดมาจากโรงงานผู้ผลิตอีเธอร์เนตฮาร์ดแวร์ ซึ่งหมายความว่า ถ้าอีเธอร์เนตฮาร์ดแวร์ของสถานีใดมีความเสียหายเกิดขึ้น (ฮาร์ดแวร์พัง) ก็เท่ากับว่าอีเธอร์เนตแอดเดรสนั้นก็สูญเสียไปด้วย เมื่อมีการนำอีเธอร์เนตฮาร์ดแวร์ใหม่มาติดตั้ง อีเธอร์เนตแอดเดรสนั้นก็ย่อมเป็นหมายเลขใหม่ด้วยเช่นกัน

ท่านผู้อ่านอาจจะมีคำถามว่าแล้วแอดเดรสนี้ใครเป็นผู้กำหนดและมีข้อปลีกย่อยอื่นอีกหรือไม่ คำตอบก็คือ ผู้ที่กำหนดแอดเดรสนี้คือสมาคม IEEE (The Institute of Electrical and Electronics Engineers) แอดเดรสนี้ถูกแบ่งเป็น 2 ส่วน แต่ละส่วนมีขนาด 3 ไบต์ โดย IEEE เป็นผู้กำหนด 3 ไบต์บน ส่วนที่เหลืออีก 3 ไบต์ล่างผู้ใช้สามารถกำหนดเองได้ตามใจปรารถนา ซึ่งสามารถกำหนดได้ถึง 2^{24} หมายเลขที่ไม่ซ้ำกัน ดังนั้นผู้ที่ต้องการจะผลิตฮาร์ดแวร์อีเธอร์เนตจะต้องขอซื้อบล็อกแอดเดรสจาก IEEE ในราคาประมาณ US$1,000 ต่อ 1 บล็อกถ้าผู้อ่านมีเครื่องมือที่เรียกว่า LAN analyzer และสังเกตดูจากการตรวจจับอีเธอร์เนตเฟรมในระบบจะพบว่าเครื่อง SUN จะมีแอดเดรสนำหน้าเป็น $(080020)_H$ cisco router มีแอดเดรสนำหน้าเป็น $(00000c)_H$ เป็นต้น

สำหรับประเทศไทยนั้นทางศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ได้ซื้อบล็อกแอดเดรสนี้มา ซึ่งมีหมายเลข $(0020c6)_H$ ดังนั้นผู้ที่สนใจจะผลิตฮาร์ดแวร์อีเธอร์เนตสามารถติดต่อขอข้อมูลได้จากศูนย์ฯ ดังกล่าว

ข้อปลีกย่อยอย่างอื่นก็คือ IEEE กำหนด 2 บิตพิเศษขึ้นมาเพื่อใช้กำหนดเป็นแอดเดรสกลุ่มและแอดเดรสเฉพาะเรียกว่า I/G บิต (individual/group) สำหรับบิตที่ใช้กำหนดขอบเขตการใช้งานของแอดเดรสในวงกว้างและในวงแคบเรียกว่า G/L บิต (global/local) ดังแสดงในรูปที่ 3 ถ้าบิต I/G เป็น "0" หมายถึง

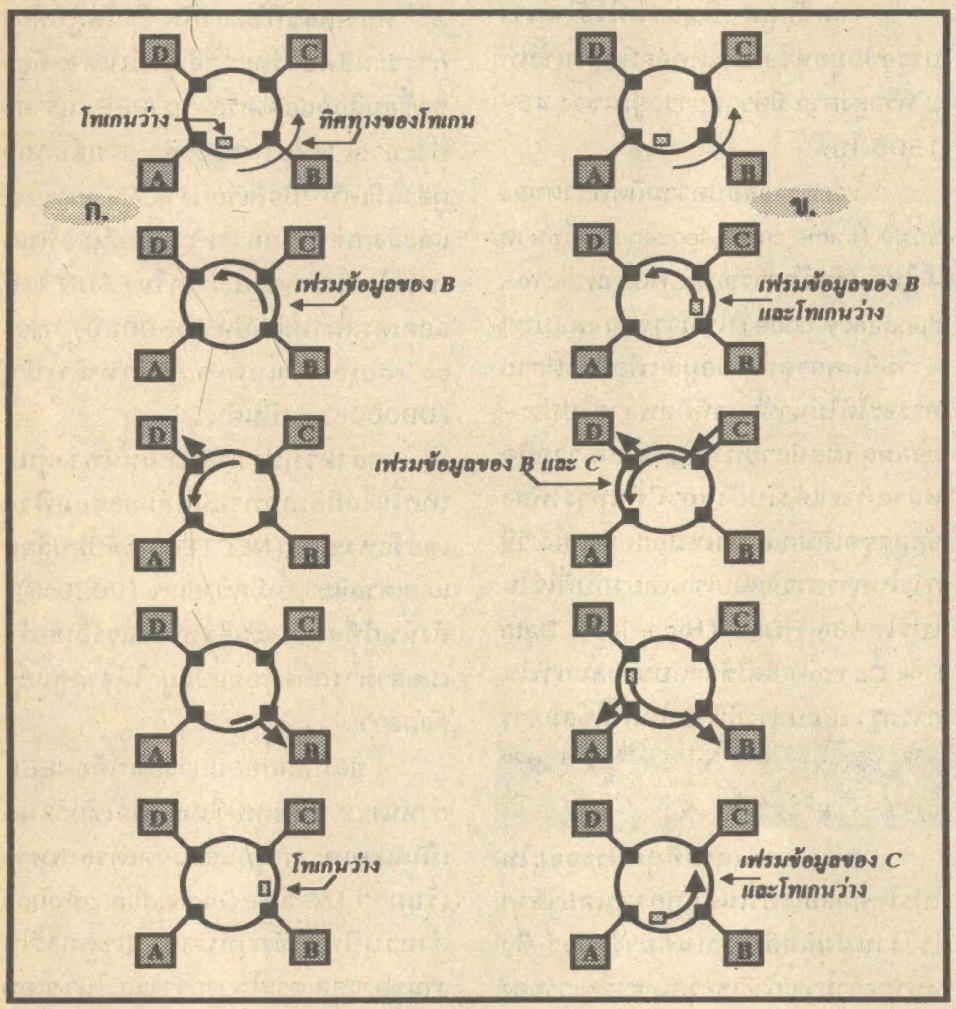
เป็นแอดเดรสเฉพาะของแต่ละสถานี แต่ถ้ามีค่าเป็น "1" หมายถึงเป็นแอดเดรสกลุ่ม (multicast address) ซึ่งใช้ในการกำหนดกลุ่มของสถานีในการรับส่งข้อมูล (ท่านผู้อ่านอย่าสับสนกับแอดเดรสกระจายข่าว เพราะแอดเดรสนี้ใช้กับทุก ๆ สถานีภายในระบบ) ถ้าบิต G/L มีค่าเป็น "0" หมายถึงเป็นแอดเดรสเฉพาะเจาะจงและรับประกันว่าทั่วโลกจะไม่มีแอดเดรสซ้ำกันโดยเด็ดขาด แต่ถ้ามีค่าเป็น "1" หมายถึงผู้บริหารระบบเครือข่ายสามารถเลือกอีเธอร์เนตแอดเดรสใช้ได้ตามใจชอบภายในระบบแลนหนึ่ง ๆ และต้องระวังการซ้ำของแอดเดรสที่อาจจะเกิดขึ้นเนื่องจากการกำหนดค่าซ้ำกันเองภายในระบบ



รูปที่ 3
ตำแหน่งของ G/L และ I/G บิต
ในเขตแอดเดรสที่ใบต์สูงสุด

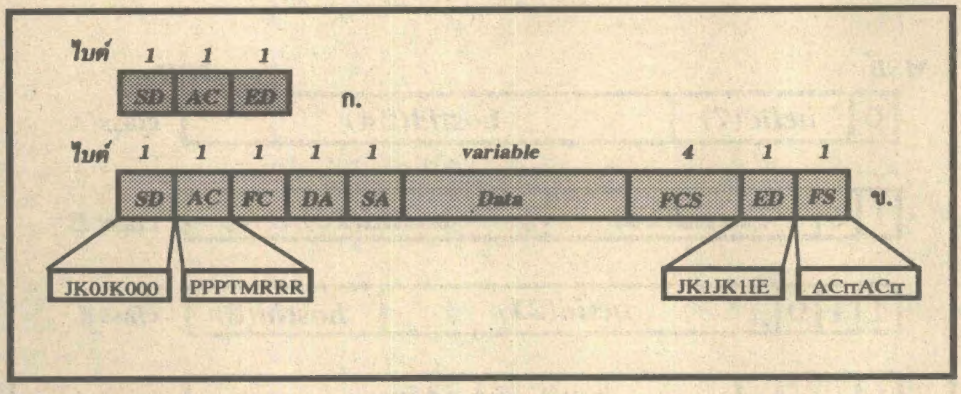
โทเก้นริงแลน

วิธีการในการเข้าใช้ช่องสัญญาณของแลนประเภทนี้เป็นแบบการตรวจจับโทเก้นเฟรม ดังแสดงในรูปที่ 4 กล่าวคือ ภายในระบบโทเก้นริงต้องมีการกำหนดสถานีพิเศษที่เรียกว่า สถานีตรวจสอบระบบ (monitor station) สถานีนี้รับผิดชอบในการควบคุมดูแลความสงบเรียบร้อยภายในแลน ขณะที่ระบบไม่มีการใช้งาน จะมีเฟรมโทเก้นว่าง (free token frame) 1 เฟรม (ซึ่งถูกปล่อยออกมาจากสถานีตรวจสอบระบบ) วิ่งวนอยู่ในระบบ (จากสถานีหนึ่งไปยังสถานีข้างเคียงจนครบรอบ) ถ้าสถานีใดต้องการส่งข้อมูลก็จะจับโทเก้นว่างนี้ไว้และเปลี่ยนเป็นเฟรมโทเก้นไม่ว่าง (busy token frame) ซึ่งภายในบรรจุข้อมูลที่ต้องการจะส่ง เมื่อข้อมูลไปถึงสถานีปลายทาง สถานีนั้นก็ทำการสำเนาข้อมูลไว้และปล่อยให้ข้อมูลเดิมวนกลับมายังสถานีที่ส่งข้อมูล และสถานีต้นทางนี้เองที่จะต้องตรวจสอบเฟรมข้อมูลที่มันส่งออกไป พร้อม ๆ กับดึงข้อมูลออกจากระบบจนหมด หลังจากนั้นก็ปล่อยโทเก้นว่างลงสู่ระบบตามเดิมเพื่อให้สถานีอื่นมีโอกาสส่งผ่านข้อมูลต่อไป



รูปที่ 4 ก. โทเก้นริงแบบ 4 เมกะบิตต่อวินาที
ข. โทเก้นริงแบบ 16 เมกะบิตต่อวินาที

วิธีการที่กล่าวมานี้ใช้กับโทเก้นริงที่มีอัตราเร็วในการส่งผ่านข้อมูล 4 เมกะบิตต่อวินาที สำหรับโทเก้นริงแบบ 16 เมกะบิตต่อวินาทีมีข้อแตกต่างในการเข้าใช้ช่องสัญญาณอยู่เล็กน้อยคือ โทเก้นริงแบบ 4 เมกะบิตยอมให้มีการส่งผ่านข้อมูลครั้งละ 1 เฟรมเท่านั้น แต่แบบ 16 เมกะบิตยอมให้มีการส่งผ่านข้อมูลครั้งละหลายเฟรมโดยวิธีการง่าย ๆ คือ หลังจากที่สถานีต้นทางส่งข้อมูลออกไปแล้ว ในส่วนท้ายของเฟรมข้อมูลต้องต่อท้ายด้วยโทเก้นว่างเสมอ ดังนั้นเมื่อเฟรมประเภทนี้ผ่านไปยังสถานีข้างเคียงใด ๆ สถานีนั้นก็สามารถส่งข้อมูลได้ทันทีโดยใช้วิธีการส่งข้อมูลเหมือนกับสถานีข้างต้นที่กล่าวมาแล้ว และต่อท้ายด้วยโทเก้นว่างเช่นเดียวกัน โทเก้นริงแบบ 16 เมกะบิตนิยมนำมา



รูปที่ 5 ก.เฟรมโทเก้นว่าง
ข. เฟรมโทเก้นไม่ว่างหรือเฟรมข้อมูล

ใช้เป็นเครือข่ายกระดูกสันหลัง (backbone network) เพราะมีสมรรถนะในการรับส่งข้อมูลดีกว่าแบบ 4 เมกะบิต สำหรับรูปแบบของโทเก้นเฟรมแสดงในรูปที่ 5

เขตเริ่มต้น (starting delimiter) มีรหัสคงที่คือ JK0JK000 "JK" เป็นรหัสพิเศษที่แตกต่างไปจากรหัสปกติ โดยใช้เทคนิค code violation เพื่อแสดงให้สถานีรับข้อมูลทราบว่าเป็นจุดเริ่มต้นของเฟรม

เขตควบคุมการเข้าใช้สื่อนำสัญญาณ (access control) แบ่งออกเป็น 4 เขตย่อยคือ

● เขตย่อย P บิต มีขนาด 3 บิต ใช้แสดงถึงศักดิ์ศรีของโทเก้นเฟรม (เลขมากหมายถึงมีศักดิ์ศรีสูง) เมื่ออยู่ในโทเก้นว่างแสดงถึงว่า สถานีใดที่ต้องการใช้ช่องสัญญาณต้องมีศักดิ์ศรีสูงกว่าหรือเท่ากับที่ถูกกำหนดไว้ในเขตย่อยนี้

● เขตย่อย T บิต มีขนาด 1 บิต ถ้ามีค่าเป็น "0" หมายถึงโทเก้นว่าง และถ้าเป็น "1" หมายถึงโทเก้นไม่ว่าง สถานีใดที่ต้องการส่งข้อมูลเมื่อพบบิตนี้เป็น "0" ก็จะเปลี่ยนให้เป็น "1"

● เขตย่อย M บิต มีขนาด 1 บิต ใช้สำหรับสถานีตรวจสอบระบบเพื่อตรวจสอบดูว่าเฟรมข้อมูลที่มันรับได้เป็นเฟรมข้อมูลใหม่หรือเฟรมข้อมูลเดิม ถ้าเป็นเฟรมข้อมูลเดิม (บิตนี้มีค่าเป็น "1") มันจะทำการดึงเฟรมนี้ออกจากระบบโดยไม่คำนึงถึงสถานีที่เป็นผู้ส่งเฟรมออกมา แต่ถ้าเป็นเฟรมข้อมูลใหม่ (บิตนี้มีค่าเป็น "0") สถานีตรวจสอบระบบจะเปลี่ยนให้เป็น "1" เพื่อแสดงว่าเคยผ่านมันไปแล้ว 1 ครั้ง และที่ต้องกระทำเช่นนี้ก็เพราะว่าถ้าสถานีส่งเฟรมข้อมูลไม่อยู่ในสภาวะที่ทำงานได้ก่อนที่จะมีการดึงเฟรมของตัวมันเองออกจากระบบ เฟรมนี้ก็ยังคงวนอยู่ในริงตลอดกาล

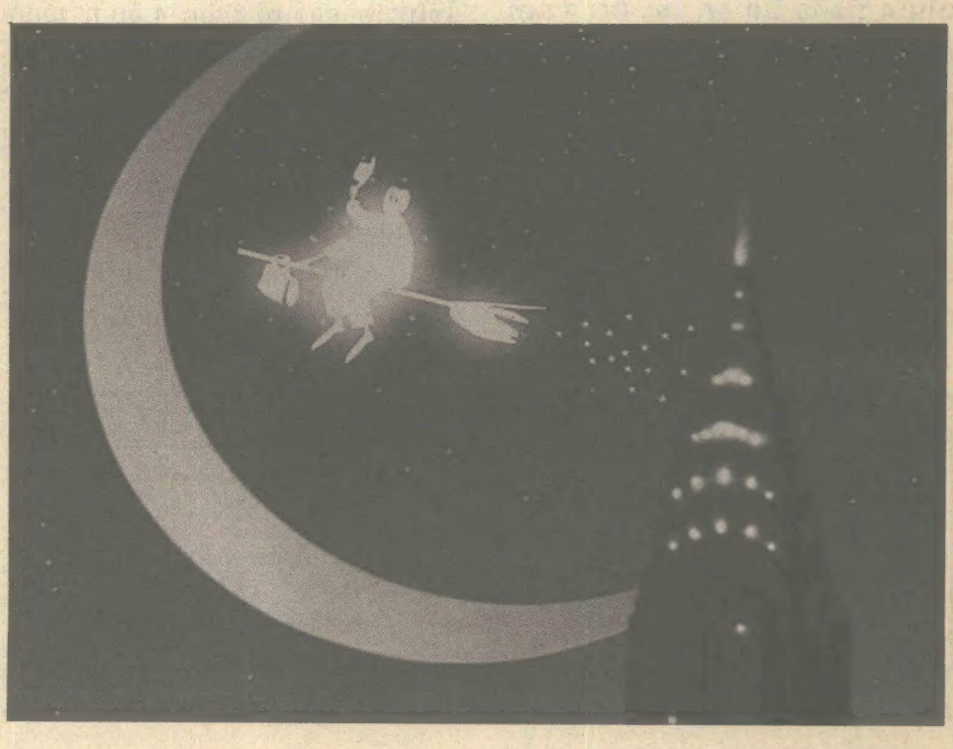
● เขตย่อย R บิต มีขนาด 3 บิต ใช้สำหรับสถานีที่มีความเร่งด่วนในการใช้ช่องสัญญาณ สามารถกำหนดศักดิ์ศรีของสถานีลงไปได้ และถ้าศักดิ์ศรีนี้ถูกปรากฏในเขตย่อย P บิตของโทเก้นว่างเมื่อใดสถานีที่ทำการจองช่องสัญญาณไว้ก็สามารถเข้าใช้ช่องสัญญาณได้ทันที

เขตเฟรมควบคุม (frame control) ใช้แสดงว่าเป็นเฟรมควบคุมการทำงานของระบบหรือเฟรมข้อมูล

เขตแอดเดรสต้นทางและปลายทาง (source & destination address) มีวัตถุประสงค์ในการใช้งานและข้อกำหนดเช่นเดียวกับอีเธอร์เนตแลน

เขตข้อมูล ใช้ในการบรรจุข้อมูลหรือโปรโตคอลที่อยู่ในชั้นที่ 2 หรือสูงกว่า ความยาวของเขตนี้ขึ้นอยู่กับช่วงเวลาที่อนุญาติให้สถานีใด ๆ มีสิทธิ์ในการส่งข้อมูล โดยปกติกำหนดไว้ที่ 10 มิลลิวินาที

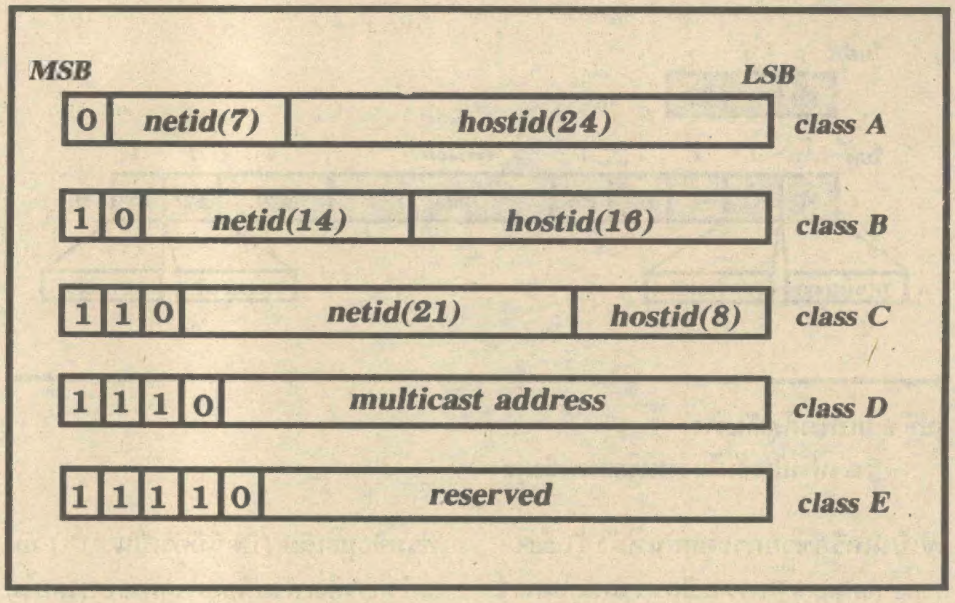
เขตตรวจสอบความผิดพลาดของ



ข้อมูล ใช้วิธีการและสมการเดียวกับอีเธอร์เนตแลน

เขตปิดท้ายเฟรม (ending delimiter) ใช้ในการบอกถึงจุดสิ้นสุดของเฟรม มีรหัสคงที่คือ JK1JK1IE "JK"เป็นรหัสเดียวกับที่ใช้ในเขตเริ่มต้นเฟรม ส่วน I และ E บิตมีที่ใช้ดังนี้คือ ถ้าเป็นโทเก้นว่างสองบิตนี้มีค่าเป็น "00" แต่ถ้าอยู่ในเฟรมข้อมูลบิต I มีค่าเป็น "1" ก็ต่อเมื่อเฟรมนั้นเป็นเฟรมแรกหรือเฟรมต่อ ๆ มาในลำดับของเฟรมทั้งหมด ยกเว้นเฟรมสุดท้ายบิต I จะมีค่าเป็น "0" นอกจากนี้แล้วบิต I จะมีค่าเป็น "0" ในกรณีที่เฟรมข้อมูลนั้นเป็นเฟรมเดียวโดด ๆ สำหรับบิต E จะมีค่าเป็น "0" เมื่อถูกปล่อยออกมาจากสถานีส่งข้อมูล ถ้าระหว่างทางมีสถานีใดตรวจพบความผิดพลาดของเฟรมดังกล่าว (อาจจะตรวจพบโดยการตรวจสอบ FCS) ก็จะเปลี่ยนบิตนี้ให้เป็น "1" เพื่อแจ้งต่อสถานีต้นทาง

เขตบอกสถานะเฟรม (frame status) มีขนาด 8 บิต แบ่งบิตใช้งานออกเป็น 4 บิตคือ บิต AA และ CC ส่วนที่เหลืออีก 4 บิตสำรองไว้ใช้งานในอนาคต ความหมายของบิต "A" และ "C" แสดงในตารางที่ 1 สาเหตุที่มีอย่างละ 2 บิตก็เพื่อป้องกันความผิดพลาดที่จะเกิดขึ้น บิต "A" และ "C" นี้เมื่อถูกปล่อยออกมาจากสถานีต้นทางจะมีค่าเป็น "0000" และถูกเปลี่ยนค่าโดยสถานีปลายทาง



รูปที่ 6 IP แอดเดรสทั้ง 5 ประเภท

IP แอดเดรส

จากที่กล่าวมาแล้ว ท่านผู้อ่านอาจมีคำถามว่า ในเมื่อโปรโตคอลชั้นที่สองมีส่วนของแอดเดรสที่ใช้ในการอ้างถึงสถานีต้นทางและปลายทางอยู่แล้ว ทำไมเราจึงใช้โปรโตคอลชั้นที่ 3 และ 4 อีก การออกแบบระบบเครือข่ายที่ดีนั้นจำเป็นต้องวิเคราะห์หลายประเด็นร่วมกัน แต่ถ้าจะกล่าวในหัวข้อของแอดเดรสนั้น ความแตกต่างระหว่าง IP แอดเดรสกับอีเธอร์เนตแอดเดรสมีดังนี้

- IP แอดเดรสสามารถทำให้ผู้ใช้งานมองระบบเครือข่ายเสมือนเป็นระบบเครือข่ายเดียวกันได้

-IP แอดเดรสมีวัตถุประสงค์ให้ผู้ใช้งานสามารถกำหนดแอดเดรสของสถานีได้ตามต้องการ

-IP แอดเดรสเป็นแอดเดรสประเภทลำดับชั้น (hierarchy) ทำให้ง่ายต่อการบริหารระบบ

-IP แอดเดรสเหมาะกับการใช้งานในระบบเครือข่ายขนาดเล็กและใหญ่

-IP แอดเดรสเป็นหัวใจสำคัญของโปรโตคอล IP เพราะเป็นแอดเดรสที่บ่งบอกถึงสถานีปลายทางจริง ๆ ภายในระบบเครือข่ายขนาดใหญ่ที่มีการเชื่อมต่อทั้ง LAN และ WAN ก่อนที่จะกล่าวถึงรายละเอียดของโปรโตคอล IP ก็ขออนุญาตทำความเข้าใจกับ IP แอดเดรสบางส่วนเสียก่อน

IP แอดเดรสเป็นแอดเดรสขนาด 32 บิต แบ่งออกเป็น 5 ประเภทดังแสดงในรูปที่ 6 คือประเภท A, B, C,D และ E แอดเดรสที่ใช้งานโดยทั่วไป(กำหนดเป็นแอดเดรสของสถานี (host)) คือ 3 ประ-

A C	ความหมาย
0 0	สถานีปลายทางที่ต้องการไม่มีอยู่ในระบบและไม่ได้รับข้อมูล
1 0	มีสถานีปลายทางที่ต้องการอยู่ในระบบ แต่สถานีนั้นไม่สามารถสำเนาข้อมูลได้
1 1	มีสถานีปลายทางที่ต้องการอยู่ในระบบ และสถานีนั้นสามารถสำเนาข้อมูลได้

ตารางที่ 1 ความหมายและความเป็นไปได้ของบิต "A" และ "C"

เภทแรก ประเภทที่ 4 ใช้ในกรณีพิเศษ ซึ่งไม่ขอกล่าวรายละเอียดในที่นี้ ส่วนประเภทสุดท้ายสำรองไว้ใช้ในอนาคต ในที่นี้ขอกล่าวเฉพาะ 3 ประเภทแรกเท่านั้น ถ้าท่านผู้อ่านคุ้นเคยกับการอ้างหน่วยความจำของหน่วยประมวลผลกลางขนาด 32 บิตจะทำให้ง่ายต่อการเข้าใจ IP แอดเดรสมากขึ้น ดังแสดงในรูปที่ 7

IP แอดเดรสแต่ละประเภทมีหมายเลขที่ไม่ซ้ำกัน ซึ่งก็หมายความว่า ถ้ากำหนดสถานีใด ๆ ด้วย IP แอดเดรส หมายเลขของสถานีก็ไม่ซ้ำด้วยเช่นกัน เมื่อมองแค่ 3 ประเภทแรกจะเห็นได้ว่าภายในแอดเดรสขนาด 32 บิตแบ่งออกเป็น 2 ส่วนย่อยคือ หมายเลขเครือข่าย (network identification (netid) และหมายเลขสถานี (host identification (hostid)) แต่ละประเภทมีขนาด netid และ hostid ไม่เท่ากัน ประเภท A มี netid ขนาด 7 บิต แต่มี hostid มากถึง 24 บิต ซึ่งแตกต่างจากประเภท C ที่มี netid ขนาด 21 บิต แต่มี hostid เพียง 8 บิต ซึ่งหมายความว่าประเภท A เน้นที่ hostid จำนวนมาก แต่ประเภท C กลับเน้นที่ netid จำนวนมาก ทำไมต้องมีการแบ่งเช่นนี้ด้วย คงจะเป็นข้อกังขาสำหรับท่านผู้อ่านหลายท่าน ซึ่งผู้เขียนขออธิบายในภายหลัง แต่ตอนนี้ขอกล่าวถึงบางส่วนของ IP แอดเดรสให้จบเสียก่อน

เพื่อความง่ายในการอ่าน/เขียน IP แอดเดรส แทนที่จะมองเป็นเลขฐานสองกลับมองเป็นเลขฐานสิบ โดยการแบ่ง 32 บิตออกเป็น 4 ไบต์ย่อย แต่ละไบต์แทนด้วยเลขฐานสิบ 1 ตัว เรียกวิธีการเช่นนี้ว่า "dotted decimal" ดังนั้นเลขแต่ละตัวของ IP แอดเดรสมีค่า 0-255 เช่น $(10011110\ 01101100\ 00000100\ 11100010)_B$ เขียนในรูป "dotted decimal" ได้เป็น 158.108.4.226 เมื่อกล่าวถึงเฉพาะ netid ของ IP แอดเดรสประเภท A, B และ C จะใช้เลขฐานสิบจำนวน 1, 2 และ 3 หลักในการอ้างถึงตามลำดับ และปล่อยให้ส่วนที่เป็น hostid มีค่าเป็น "0" เช่น 1.0.0.0, 158.108.0.0 และ 195.200.10.0 เป็น netid ประเภท A, B และ C ตามลำดับ

0000000 ..... 00000 : 0111111 11111	CLASS A
1000000 ..... 00000 : 1011111 11111	CLASS B
1100000 ..... 00000 : 1101111 11111	CLASS C
1110000 ..... 00000 : 1110111 11111	CLASS D
1111000 ..... 00000 : 1111011 11111	CLASS E

รูปที่ 7 ช่วงของ IP แอดเดรสแต่ละประเภท

การนำ IP แอดเดรสมากำหนดเป็นหมายเลขของเครือข่ายหรือสถานีนั้นมีข้อกำหนดปลีกย่อยอยู่หลายประการ ซึ่งผู้วางระบบจำเป็นต้องเข้าใจในส่วนนี้จึงจะกำหนดแอดเดรสในการใช้งานได้ไม่ผิดพลาด ข้อปลีกย่อยที่กล่าวถึงมีดังนี้

- IP แอดเดรสที่เป็น "0" หมดทุกบิตไม่มีการนำไปใช้งานทั่วไป เว้นแต่จะใช้ในอุปกรณ์หาเส้นทาง (router) เพื่อกำหนดเป็น "default route" เท่านั้น เช่น "ip route 0.0.0.0 0.0.0.0 192.150.250.9"

- ในส่วนของ netid และ hostid จะเป็น "0" หรือ "1" หมดทุกบิตไม่ได้ เช่น แอดเดรสประเภท B สามารถกำหนดเป็นอะไรก็ได้ตั้งแต่ 128.1.0.0 - 191.254.0.0 แต่จะไม่มี 128.0.0.0 และ 191.255.0.0 โดยเด็ดขาด

- หมายเลขของ netid ที่ถูกนำไปใช้งานได้ถ้าส่วนของ hostid เป็น "0" หมดทุกบิต หมายถึงหมายเลขของเครือข่ายเท่านั้น หมายเลขนี้มีประโยชน์ในการใช้งานร่วมกับอุปกรณ์หาเส้นทาง หรือใช้บอกให้สถานีรู้ว่าตัวมันเองอยู่สังกัดเครือข่ายใด

- หมายเลขของ netid ที่ถูกนำไปใช้งานได้ถ้าส่วนของ hostid เป็น "1"

	class A	class B	class C
netid	1.0.0.0 - 126.0.0.0	128.1.0.0 - 191.254.0.0	192.0.1.0 - 223.255.254.0
hostid	x.0.0.1 - x.255.255.254	x.x.0.1 - x.x.255.254	x.x.x.1 - x.x.x.254
netmask	255.0.0.0	255.255.0.0	255.255.255.0
จำนวน host	2^{24}-2	2^{16}-2	2^{8}-2

ตารางที่ 2 IP แอดเดรสและจำนวน host ที่ใช้งานได้

หมดทุกบิต หมายถึงแอดเดรสที่ใช้ในการกระจายข่าว (broadcast address) ภายในหมายเลขเครือข่ายนั้น ๆ

- IP แอดเดรสที่มีส่วนของ netid และ hostid เป็น "1" หมดทุกบิต หมายถึงแอดเดรสที่ใช้ในการกระจายข่าวเช่นกัน แต่ในกรณีนี้สามารถสรุปได้ว่าสถานีที่ปล่อยแอดเดรสเช่นนี้ลงในระบบไม่ทราบว่าตัวมันเองอยู่ใน netid หมายเลขใด

- เฉพาะ IP แอดเดรสประเภท A ที่มีหมายเลข netid เป็น 127.0.0.0 ถูกสงวนไว้ใช้งานเฉพาะอย่างเท่านั้น เช่น IPC (Inter-Process Communication)

การกล่าวถึง IP แอดเดรสให้ถูกต้องจำเป็นต้องกล่าวถึง "network mask (netmask)" ควบคู่ไปด้วย แน่นอน! คำถามที่เกิดขึ้นในขณะนี้ก็คือ netmask คืออะไร

netmask มีขนาด 32 บิต และนิยมอ่าน/เขียนในรูปของ "dotted decimal" เช่นเดียวกับ IP แอดเดรส ใช้ในการชี้ชัดลงไปว่า netid หมายเลขหนึ่ง ๆ ถูกแบ่งออกเป็นเครือข่ายย่อย (subnetwork) หรือไม่ (รายละเอียดการแบ่งเครือข่ายย่อยไม่ขอกล่าวในที่นี้ และในบทความนี้จะกล่าวเฉพาะ netid ที่ไม่ถูกแบ่งเป็นเครือข่ายย่อย) ถ้าไม่มีการแบ่งเป็นเครือข่ายย่อยจะแทนในส่วนที่ตรงกับประเภทของ netid ด้วยเลข "255" เสมอ เช่น IP แอดเดรสประเภท B หมายเลข 158.108.0.0 มี netmask เป็น 255.255.0.0, IP แอดเดรสประเภท A หมายเลข 1.0.0.0 มี netmask เป็น 255.0.0.0 เป็นต้น

จากรายละเอียดของ IP แอดเดรสและ netmask ดังกล่าวข้างต้นสามารถสรุปหมายเลขของ netid, hostid และ netmask ที่ถูกนำมาใช้งานได้จริง ๆ ดังตารางที่ 2

สรุปก่อนจาก

มาถึงจุดนี้ท่านผู้อ่านคงจะได้เห็นรายละเอียดของโปรโตคอลอีเธอร์เนต โทเก้นริง และ IP แอดเดรสพอสมควร บางท่านอาจจะมองเห็นความสัมพันธ์แล้ว แต่บางท่านอาจจะยังงงอยู่ ถ้าเป็นประการหลังก็คงต้องอ่านซ้ำอีกสักครั้งหรือสองครั้งเพื่อจะได้เข้าใจและจดจำรูปแบบของมันได้

ในฉบับหน้าซึ่งเป็นตอนจบของบทความนี้ จะเห็นได้ว่างานประยุกต์สามารถถูกเชื่อมโยงเข้าหากันโดยใช้ชุดโปรโตคอล TCP/IP ได้อย่างไร และการเลือกใช้ชุดโปรโตคอลที่ประกอบด้วยโปรโตคอลชั้นที่ 3 นั้นดีอย่างไร

เอกสารอ้างอิง

1. เขมะทัต วิภาตะวนิช, มารู้จักมาตรฐานระบบเครือข่ายคอมพิวเตอร์, ไมโครคอมพิวเตอร์, ฉบับที่ 81, เมษายน, 2535.
2. Halsall F., Datacommunications, Computer Networks and Opensystems, 3rded., Addison Wesley, Massachusetts, 1992.
3. Comer D.E., Internetworking with TCP/IP vol.1, 2nded., PHI, New Jersey, 1991.